

上海天好证券行业大数据平台红帽联合

容器云解决方案白皮书

2021 容器云
职业技能大赛

聚力变现容器价值
开放从容不凡



目录

1. 概述 4
2. 背景 5
  2.1 政策背景......5
  2.2 行业背景......5
3. 金融科技创新在证券行业的影响与实践 6
  3.1 证券公司数字化转型不断加速......6
  3.2 券商金融科技的实践探索......7
    3.2.1 经纪业务领域 7
    3.2.2 投行业务领域 8
    3.2.3 资管和自营业务领域......8
4. 天好大数据平台......9
  4.1 大数据数据处理管理平台......9
  4.2 天好大数据数据质量管理平台......10
  4.3 天好大数据数据资产管理平台......11
  4.4 天好大数据数据治理平台......12
  4.5 天好大数据数据分析平台......13
  4.6 天好大数据 API 管理平台......14
  4.7 天好 AI 人工智能平台 15
5. 容器云的特点 16
6. 应用场景......17
7. 方案整体设计 18
  7.1 物理部署架构 18
  7.2 逻辑架构......18
  7.3 容器编排......20
  7.4 网络模型......21
    7.4.1 OpenShift SDN 基本概念......21

7.5 存储规划......22
7.5.1 OpenShift 存储管理方案......22
7.6 ROOK 的特性......23
7.6.1 OpenShift 容器平台部署 Rook......24
7.6.2 Rook 架构......24
8. 方案特点介绍......25
8.1 云原生应用平台......25
8.2 容器技术标准化......25
8.3 弹性伸缩......26
8.4 应用编排......26
8.5 容器存储......27
8.6 集群高可用性......28
8.7 监控告警......29
8.8 日志收集......29
8.9 DevOps......30
8.10 OpenShift 自动构建应用......31
9. 关于上海天好......33
9.1 公司简介......33
9.2 公司产品......34
9.3 公司主页......35
10. 关于红帽公司......35
10.1 公司简介......35
10.2 发展历程......36



1. 概述

国内证券行业竞争日益剧烈，证券公司不仅要面临行业内的激烈竞争，还要面临来自其他金融机构、互联网公司和外资金融机构的多重竞争。证券公司为应对挑战和保持竞争力，必须实现业务快速发展和不断创新，这就需要借助金融科技的力量，提升研发主动性、灵活性和专业性，实现从 " 以项目为中心 " 到 " 以产品为中心 "、向敏捷转型。随着大数据、容器云、人工智能等新兴技术在金融行业的广泛应用，证券公司也在不同业务领域实践和探索与新技术的结合，在稳扎稳打的基础上实现证券公司的数字化转型。

天好基于容器云的大数据平台是考虑证券行业特点及数字化转型诉求，利用天好多年沉淀的数据治理理念和成熟工具链，融合大数据和容器云两种新兴技术的优势构建的一站式平台，具有以下主要特色：

- 开放的大数据集成，融合，及分析体系架构；
- 多样化的数据质量检验方式、规范化数据服务方式；
- 一站式可视化研发平台；
- 与主流的大数据底层技术实现无缝兼容；
- 多源异构的数据处理、数据治理、数据资产管理、数据质量管理；
- 提供数据分析、 API 管理、 人工智能等增值功能；
- 实现数据应用的完整闭环，帮助证券公司实现业务价值。

该解决方案是基于企业级开源产品红帽 OpenShift 容器云平台为基础，作为云原生技术建设基建平台，进而研发出证券大数据管理平台的数据采集场景，利用 OpenShift 提供的源码到镜像工具灵活的构建应用，便捷的蓝绿发布，实现了大数据平台上各业务系统功能的快速迭代。



2. 背景

2.1 政策背景

中国人民银行于 2019 年 8 月发布《金融科技（FinTech）发展规划（2019-2021 年）》，为金融行业金融科技工作的应用提供了重要的指导思想、基本原则、整体发展目标和重点任务，规划明确提出金融科技赋能金融服务提质增效，合理运用金融科技手段丰富服务渠道、完善产品供给、降低服务成本、优化融资服务，提升金融服务质量与效率，使金融科技创新成果更好地惠及百姓民生，推动实体经济健康可持续发展。

《中国银行业信息科技“十三五”发展规划监管指导意见》也指出：银行业金融机构要深入贯彻落实《国务院关于促进云计算创新发展培育信息产业新业态的意见》，探索构建私有云平台，采用成熟度高、开放性强的计算虚拟化、容器虚拟化、分布式存储、网络虚拟化等技术，建立资源池，形成资源弹性供给、灵活调度和动态计量的私有云平台。

2.2 行业背景

近年来，证券公司在证券投资、客户营销、资本市场研究、券商公司治理等领域综合运用云计算、大数据、人工智能、物联网、区块链等金融科技手段，推动传统金融转型和服务模式创新，但国内证券行业面临来自其他金融机构、互联网公司和外资金融机构的多重竞争。一是资管新规实施后，银行、信托、券商资管、公募基金等资管机构在同一监管框架下开展资管业务，从过去的合作为主转向更加复杂的竞争与合作关系，特别是金融科技发展更早、投入更大且资金雄厚的大中型商业银行加入资管业务。二是互联网公司通过申请牌照、入股现有证券经营机构等方式进军证券行业，并利用其在流量、用户体验和成本等方面的优势，挑战传统证券业务模式。三是在金融业对外开放加速的大背景下，实力强大的外资投行纷纷进入中国市场，也使国内证券行业需要在科技方面跟进外资投行的发展步伐，券商需要依靠金融科技以应对挑战和保持竞争力。

在内外部高度竞争的行业市场环境下，证券公司既要满足业务快速发展和不断创新的需要，注重产品设计和用户体验，缩短产品研发上线时间，又要提升研发主动性、灵活性和专业性，实现从 " 以项目为中心 " 到 " 以产品为中心 "、面向敏捷化和持续集成的研发模式转变。各类业务，尤其是互联网创新业务，推动“开发

测试云”、“生产云”、“灾备云”等构建更敏捷灵活的研发模式和技术体系，搭建更高效的平台，以迅速响应业务和客户的需求 根据中国证券业协会对证券行业中金融科技战略及配套研发体系建设情况的专项调查，有约 50 家证券公司建设了私有云平台（包括虚拟化技术或容器技术）并在各业务领域使用。有 20 余家证券公司已建或在建容器化私有云平台， 目前总体还处于起步实践阶段。而从整个金融行业看，已有超过三成已使用云计算技术的金融机构已将容器技术用于生产环境或测试环境。

3. 金融科技创新在证券行业的影响与实践

以习近平同志为核心的党中央高度重视数字经济，习总书记指出，“世界经济数字化转型是大势所趋，要发展数字经济，应利用网络新科技对传统产业进行全角度、全方位、全链条的改造，提高全要素生产率，释放数字化对经济发展的叠加、放大及倍增作用”。

3.1 证券公司数字化转型不断加速

证券公司作为经营信用、与数字打交道的行业，数字化不仅意味着经营效率的提升，还会带来企业运营模式的变革和重塑。以大数据技术为支撑的经营决策体系、征信管理体系和客户服务体系，以人工智能为支撑的交易服务体 系、运营风控体系，正日益成为推动证券公司持续稳健发展的新动力。多种新兴金融技术的交叉运用，带来业务体系、管理模式、组织架构、运营管理的不断革新，大大改进了客户体验, 有利于解决客户痛点问题, 重构人们的金融习惯, 激发新的业务增长点。

物联网和 5G 等科技创新正在孕育新一轮金融创新。随着万物互联互通成为现实，证券公司已经具备了将自身服务渗透到各类生活场景的技术能力，能够将各类证券业务延展至新载体和新渠道，包括可穿戴设备、5G 智能手机、虚拟现实设备等，使金融服务润物细无声，触手可及，真正实现普惠化。

金融服务虽然“无形”，但却无处不在。金融服务应服务于实体经济，并有效融入生产生活场景。对于证券公司而言，一方面要适应数字化经济转型的大趋势，通过“场景 + 金融”模式，为客户提供端到端的服务；另一方面要广泛 对接第三方合作伙伴，不断拓展行业边界，打造共赢互利的金融生态圈。实现“平台 + 生态”的新型证券服务模式，将证券专业服务渗入实体经济各领域，打破原有业务间壁垒和行业进入门槛，打通贯穿实体经济和证券服务的价值链， 达到证券服务“无处不在、无微不至”。



3.2 券商金融科技的实践探索

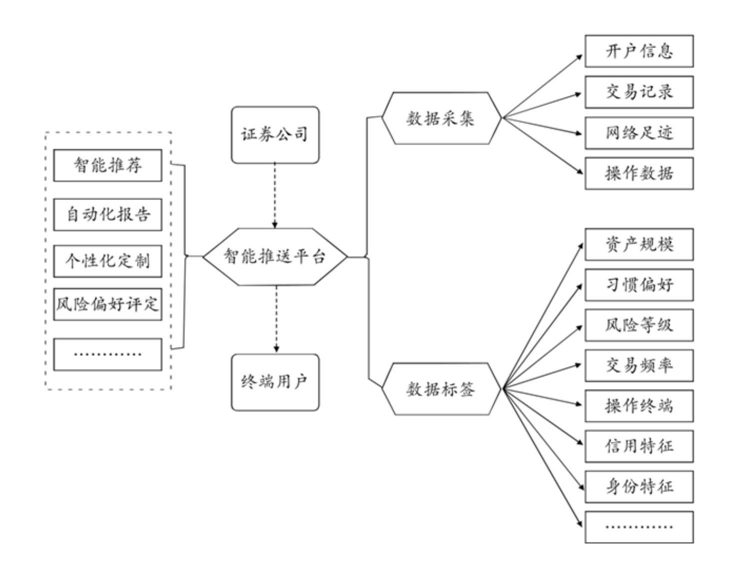
从实践层面来看，当前券商智能化和数字化的转型主要是通过券商自建金融科技业务系统或与金融科技企业开展战略合作，提升数字化服务能力，重塑经济业务、投行业务、资产管理、自营业务等行业生态。如经纪业务由发展通道向理财业务和信用中介终端转变，在业务链条拓展、风险定价实施、资产证券化等方面开辟新的盈利模式，应用场景也从传统的智能投顾、智能客户向客户画像、交易轨迹、量化方案等方向拓展。

3.2.1 经纪业务领域

金融科技有利于提升证券经纪业务的数字化、智慧化运行和服务水平，降低获客和服务成本，使得券商的经纪业务由通道业务转向财富管理。券商经纪业务领域的金融科技应用主要包括以下几方面。

- 智能开户 / 销户。在前期开户预约、适当性管理、风险测评、资料收集上传、在线销户等方面的“线上化”缩短了客户开销户办理时间，大大提升了服务效率和客户体验。

- 智能推送。金融科技能让券商 APP 更加“聪慧”。如部分券商的 APP 已经可以在客户登录交易软件时自动推送适合该客户的资讯主题和链接，并且做到“千人千面”，同时在客户不主动发起访问的情况下做到“主动推送”，包括量化策略提供、目标理财、行情推送等功能。



- 智能客服。为打造稳定的客户服务体系，目前证券业通过 AI 驱动定制化客服平台以及语音文本转换、语气识别、问题预测、问答检索及交互会话等技术， 使智能机器人能够自主与客户进行互动交流，实现智能实时监控、智能质检、智能分析等常见业务功能，从而降低客户等待时间，增加用户智能体验与安全保证， 增强用户粘性。

3.2.2 投行业务领域

一般来说，券商投行业务包括 IPO、再融资、企业重组、兼并与收购等， 在投行营销和项目承揽方面，金融科技有助于提升投行业务对“潜在机会”的捕捉， 通过增强专业数据分析能力和动态督导能力，提升业务专业水平和工作效率。在 机会挖掘方面，可利用网络爬虫等技术对海量的工商、监管、投融资、新闻资讯 等各方面信息进行整合处理，实现对资本市场产业链相关客户的挖掘，带动投行 综合化联动营销。

在业务督导和投融资服务方面，运用行业分析、产业链图谱、智能舆情监控等方面的大数据技术，实现相关企业的全方位风险评估和目标定价，实现投行业务的事后监督和管理。

此外，通过基于深度学习和自然语言处理的“文档审核”、“文档自动生成” 以及机器人流程自动化（RPA）等技术，实现投行业务数字化、电子化和自动化， 进而大幅提升投行业务效率。

3.2.3 资管和自营业务领域

券商资管和自营业务主要涉及券商通过发行资管产品或使用自有资金来投资股票、债券、衍生品等。

- 智能投顾。目前国内智能投顾的主要服务模式包括：（1）根据客户的风险属性来确定股票、债券和货币的配置比例；（2）根据市场舆情监测分析提供的主题投资策略；（3）充当股票交易型社交投资工具；（4）根据量化指标分析的量化投资策略；（5）针对海外成熟市场的全球资产配置。

- 投研服务平台。未来的投研服务平台是包含以金融预测、投资推荐、决策辅助、投顾助手、组合管理等特色的智能投研，大数据、人工智能引入后， 投研服务

平台投研服务能力会得到大幅提高，不仅对外提供咨询报告，对内也提供投研服务产品

4. 天好大数据平台

以天好云平台为基础，基于天好多年沉淀的数据治理理念和成熟工具链， 构建一站式的云大数据平台。

大数据平台是天好长期实践探索形成的平台级大数据产品，具备开放的大数据集成，融合，及分析体系架构。提供多样化的数据质量检验方式、规范化数据服务方式、一站式可视化的大数据研发平台，可与主流的大数据底层技术实现无缝兼容。平台提供多源异构的数据处理、数据治理、数据资产管理、数据质量管理、数据分析平台、API 管理平台、AI 人工智能平台等功能，为政府机构、企业、科研机构、第三方软件服务商等客户，提供大数据管理、开发和计算的能力，可支撑企业级数据仓库、用户画像、知识图谱、深度学习、文本分析、全文检索及更多企业级应用的构建。同时让客户最大化的发现与分析企业内部核心业务数据价值，挖掘现有业务和应用系统的潜在商机，培育完好的业务创新产业链，实现数据应用的完整闭环，帮助客户实现商业价值。

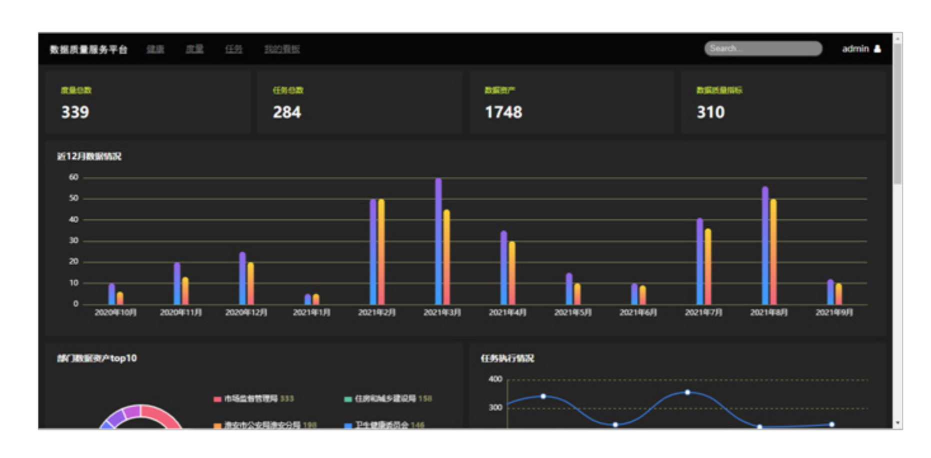
4.1 大数据数据处理管理平台

数据处理平台有着模块化的设计结构，作为一个完整的系统，它能够解决人机交互，数据的输入输出，数据处理方法管理等一系列数据处理中的关键问题。平台各个组成模块之间相互独立，在工作时互相配合，方便系统的扩展和升级。数据处理平台为数据处理模型提供支持和管理，包括模型的创建、配 置、调度执行、管理监控等。数据处理模型负责完成数据迁移、数据转换、数据筛选等数据处理相关工作。它是实际运行在用户生产环境中的实际系统，建立在数据处理平台基础之上。虽然功用可能有所不同，但是它们在系统设计方法和原则、系统架构、需要解决的关键问题、实施过程等方面具有很强的共通性。平台首先应与全系统兼容，同时应具备的主要性能包括：易操作性、实用性、安全性、可扩展性、易管理性、易维护性等。平台设计运用了软件工程的软件开发思想，经历软件定义，需求分析，软件设计，软件实现，软件维护等阶段。

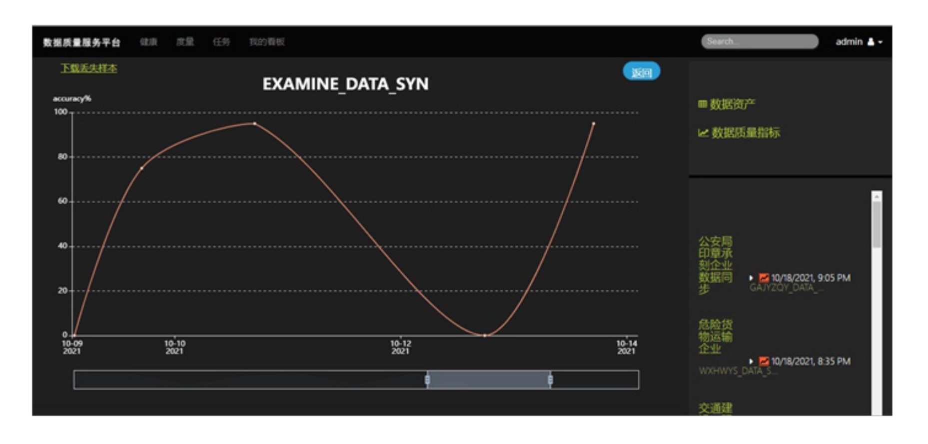


4.2 天好大数据数据质量管理平台

数据质量问题产生的因素有多个方面，主要有设计问题、传输和使用问 题、操作问题等方面。正因为数据质量产生于多个方面，因此其治理的难度不言而喻，例如：由于历史原因造成大量缺失数据和错误数据。需求考虑不周导致数据质量问题的产生。需求人员在拟定需求时，往往从当前使用场景出发， 对后续使用场景以及与其他系统之间的关联关系考虑较少，出现系统间数据不一致，当前数据业务场景使用等情况。操作不合规形成数据问题。操作人员在操作时错误或不严谨，也会导致问题产生，比如输入随意的 11 位数字用作手机号码等。数据质量管理平台提供数据质量规则的定义和管理，数据质量规则定义数据质量审核的业务逻辑，是数据质量审核和监控管理的基础。数据质量管理平台能够从设计、开发、生产等各个环节发现数据质量问题，及时进行数据治理并提炼相应的数据质量检核规则，防止同类问题的重复发生，有效提升数据整体数据质量，从而更好地为客户服务，提供更为精确的决策分析数据。





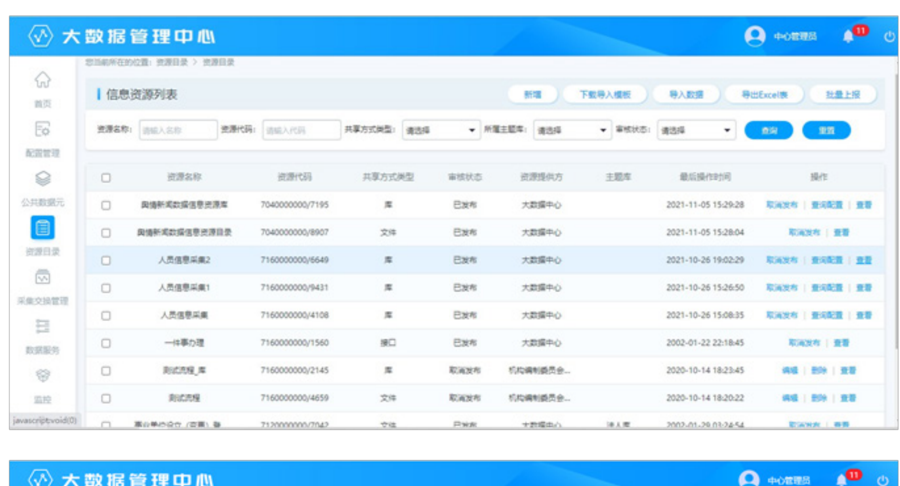


4.3 天好大数据数据资产管理平台

数据资产管理是规划、控制、和提供数据这种企业资产的一组业务职能， 包括开发、执行和监督有关数据的计划、政策、方案、项目、流程、方案和程序。企业



依赖有效数据资产管理为其提供可靠、有价值和高质量的数据，提供更好的产品和服务，降低开发和运维成本，控制风险，以及为企业提供更明智和更有效的决策数据支持。

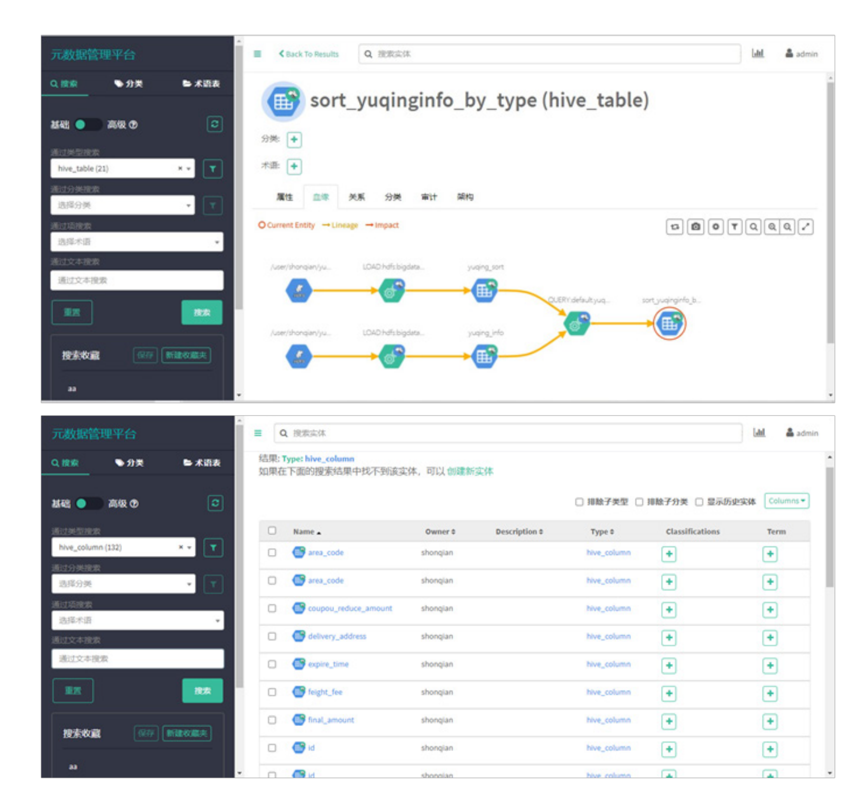




4.4 天好大数据数据治理平台

数据治理是组织中涉及数据使用的一整套管理行为。由企业数据治理部门发起并推行，关于如何制定和实施针对整个企业内部数据的商业应用和技术管理的一系列政策和流程。数据治理平台是以元数据为基础，实现数据的产生、存储、迁移、使用、归档、销毁等环节的数据生命周期管理。实现数据从源到数据中心再到应用端的全过程管理，为用户提供了准确便捷的企业资产信息。数据治理平台也包括数据标准，数据质量。



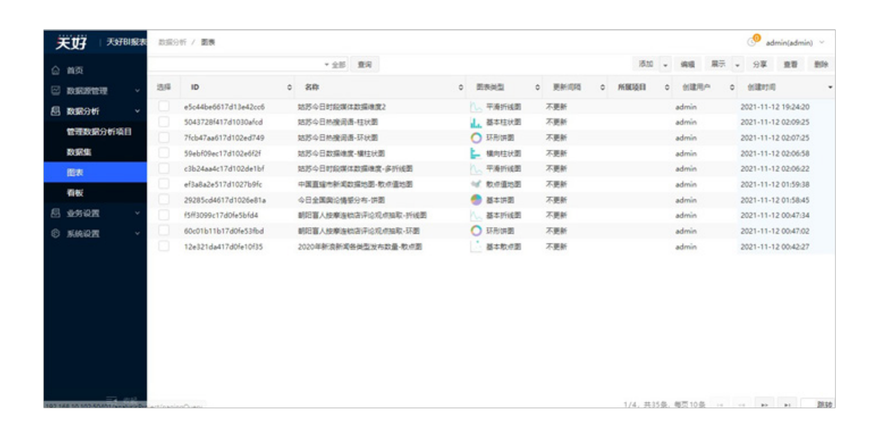


4.5 天好大数据数据分析平台

数据分析平台是由自主研发的一款全能型核心数据产品，既可以为实施人员提供面向数据仓库的数据分析展现，也可以为业务人员提供自助式数据分析能力，全方位满足用户的数据应用场景，通过丰富的数据分析手段，为用户提供一站式数据分析平台。该产品是我公司在多年数据分析、报表处理的技术经验基础上，运用先进的数据仓库、商务智能核心理论，经过多年的潜心研发而推出的商务智能产品软件，很大程度上能降低数据分析实施技术门槛，使复杂的工作简单化、重复的工作智能化。



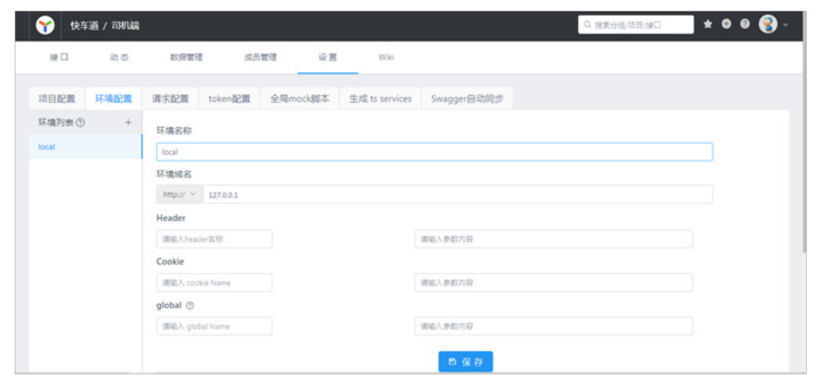




4.6 天好大数据 API 管理平台

API 管理平台，旨在为开发、产品、测试人员提供更优雅的接口管理服务。可以帮助开发者轻松创建、发布、维护 API，API 管理平台还为用户提供了优秀的交互体验，开发人员只需利用平台提供的接口数据写入工具以及简单的点击操作就可以实现接口的管理。还支持导出 API 接口等。

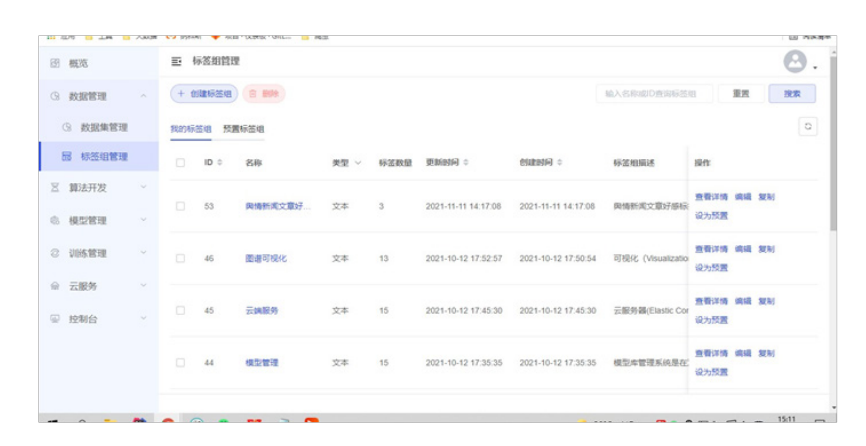




4.7 天好 AI 人工智能平台

最近几年，随着人工智能技术的快速发展，深度学习摧枯拉枯之势席卷 IT 的各个角落，改变了各领域算法研究和软件开发的模式，也给 IT 基础设施建设和平台工具研发带来了新的要求。快速搭建起一个分布式的深度学习训练平台，加速深度神经网络的训练，可以有效提高公司的竞争力。AI 人工智能平台的兴起，基于人们对于高密度、多维度、碎片化数据信息的采集、存储、计算、分析等一系列处理流程的“智能计算”需求；而“智能计算”需求的出 现，则源于科技发展所推动的人类生产力进步，和人类对于科技赋能下的更高质量生产生活的追求之间的相互作用，所催生的对于“数据”这一全新生产要素的应用。如果说数据是建立当前数字经济摩天大厦的钢筋螺母，那么智能平台则是浇筑吊装这些组件的大型工程器械，正所谓 “工欲善其事，必先利其器”，高性能、强可靠的智能平台可以极大提升大规模数据的处理效率与分析精度，令当众多大数据平台项目的建设如虎添翼。





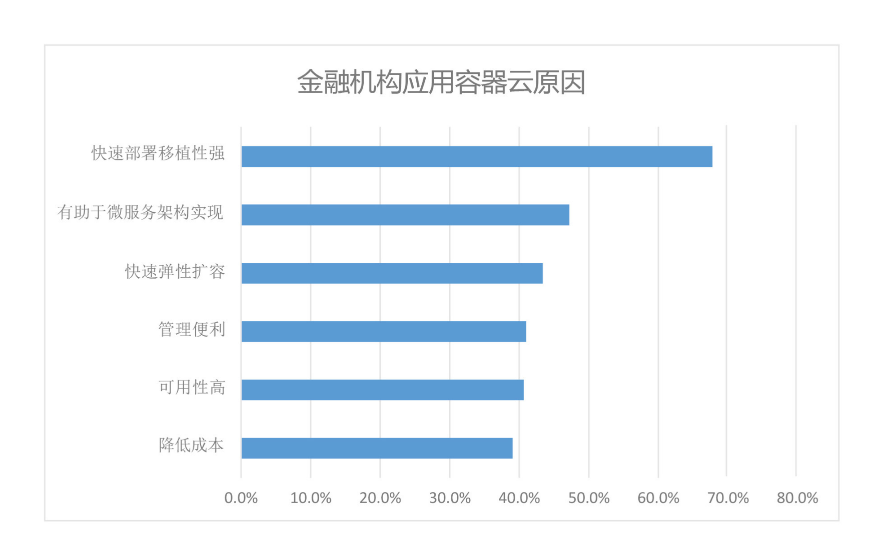


5. 容器云的特点

容器作为一种轻量级的虚拟机，和传统的虚拟机有所区别。传统的虚拟机是在宿主机的操作系统上再虚拟一整个操作系统出来，每一个虚拟机的应用不仅仅包含这个应用的类库代码（可能只有十几 MB），还包含一整个操作系统（GB 级别以上）。而容器则共享整个宿主机操作系统的资源，仅仅包含应用本身和其依赖。因此，相比之下容器显得更加便捷和高效。

容器云与虚拟化技术对比分析

	指标项	容器技术	虚拟化技术
1	操作系统	共享宿主机 OS	使用独立的 OS
2	存储空间	较小，一般为 MB 级	较大，一般为 GB 级
3	性能损耗	较少，接近原生	较多，包括 OS、应用系统等
4	可移植性	支持常见 linux 和 Windows 系统	依赖虚拟化平台
5	部署速度	快速	相对较慢
6	部署密度	几百个 / 单台服务器	几十个 / 单台服务器
7	部署内容	容器镜像	虚拟机镜像
8	启动速度	快速	相对较慢
9	稳定性	逐步更新中，	相对成熟稳定
10	安全性	采用对应技术与部署方式保证	安全，GuestOS 独立运行
11	高可用性	通过业务本身保障	虚拟化平台充分保障
12	监控成熟度	发展中	虚拟化平台监控手段成熟
13	管理成熟度	发展中	虚拟化平台管理手段成熟



根据相关调查，能够实现快速部署、有助于微服务架构的实现是金融机构应用容器技术的主要原因。已经应用容器技术的金融机构中，出于能够快速部署应用的目的而应用容器技术的金融机构最多，占比 67.8%；其次，47.2% 的金融机构认为有助于微服务架构的实现是金融机构应用容器技术的原因；另外，支持快速弹性扩容 (43.4%) 以及管理便利 (41.0%) 也是金融机构应用容器技术的重要推动力。

6. 应用场景

证券公司在应用敏捷研发模式时，其迭代周期根据具体产品和项目而不同， 一般在 2-4 周。采用敏捷研发的产品范围涉及证券经纪业务、资产管理、自营技资、固定收益、投资银行、合规风险、运营决策、系统运维八大业务领域，一般为自主研发的项目，主要集中在个性化程度较高、需要快速响应业务或市场的应用领域，如 APP 等互联网渠道应用、中后台个性化管理应用等。有些中台化程度较高的证券公司，敏捷模式也应用在中台系统开发上，如业务中台服务，以便能够快速响应并支持前端应用的开发需求。在以上微服务、DevOps、持续交付场景中，容器云均可适用。

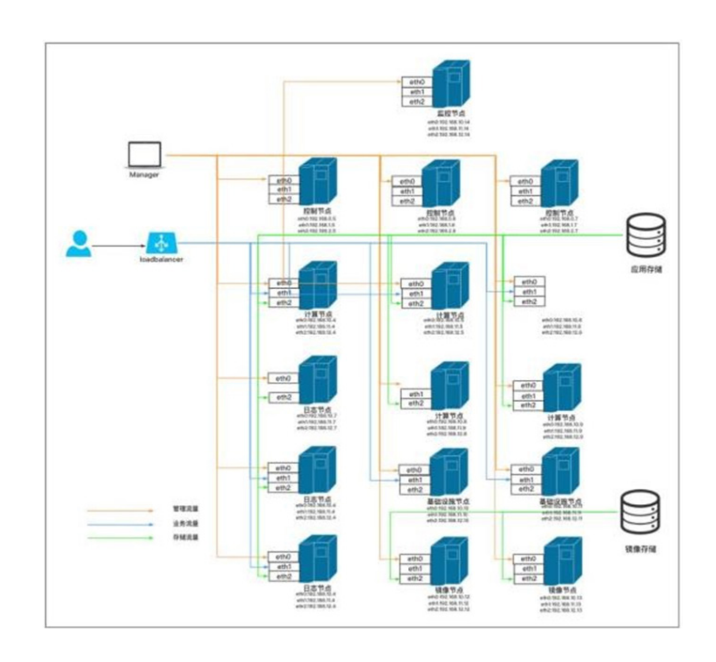
	应用	容器化	原因
微服务	API 服务	适合	微服务鼓励软件开发者将整个软件解耦为较小的功能片段，容器进一步对这种解耦性进行了扩展，它能够将软件从底层的硬件中分离出来。这种方式所产生的结果 是：应用程序能够更快地进行创建，且更易于维护，同时又能够得到更高的质量； 微服务的应用都是轻量化、无状态并且易于水平扩展
前端服务	Nginx、Apache	适合	WEB 服务和接人服务这类无状态的服务，应用程序设计的主要优点在于：它能够平稳地应对为服务添加或移除某些实例的场景，而无须对应用程序进行重大的变更或进行配置的改动。比方说，如果服务的负载产生了突发性的增长，可以为服务加入更多无状态的ｗｅｂ服务器，而如果某个无状态的服务器挂机了，也可以方便地用另外一台服务器取代它。所以此类服务更容易体现容器所带来的快速弹性调度的特性
中间件服务	Weblogic、Websphere	不推荐	一般是重资源消耗型应用
	JBoss、Tomcat、Resin	适合	一般为轻量级应用，可冗余，无状态
消息类服务	Kafka、FabbitMQ、ActiveMQ、ZeroMQ 等	不推荐	消息类服务都是有状态的服务，对消息的可靠性、传输性要求高，需要持久化，属于有状态服务。并且某些消息类组件不可冗余分割

7. 方案整体设计

本方案将在虚拟化 / 物理机基础设施之上搭建云原生应用平台，同时通过平台内置的软件定义存储系统把集群主机的离散存储汇集为存储资源池，为应用的数据持久化提供存储支持。

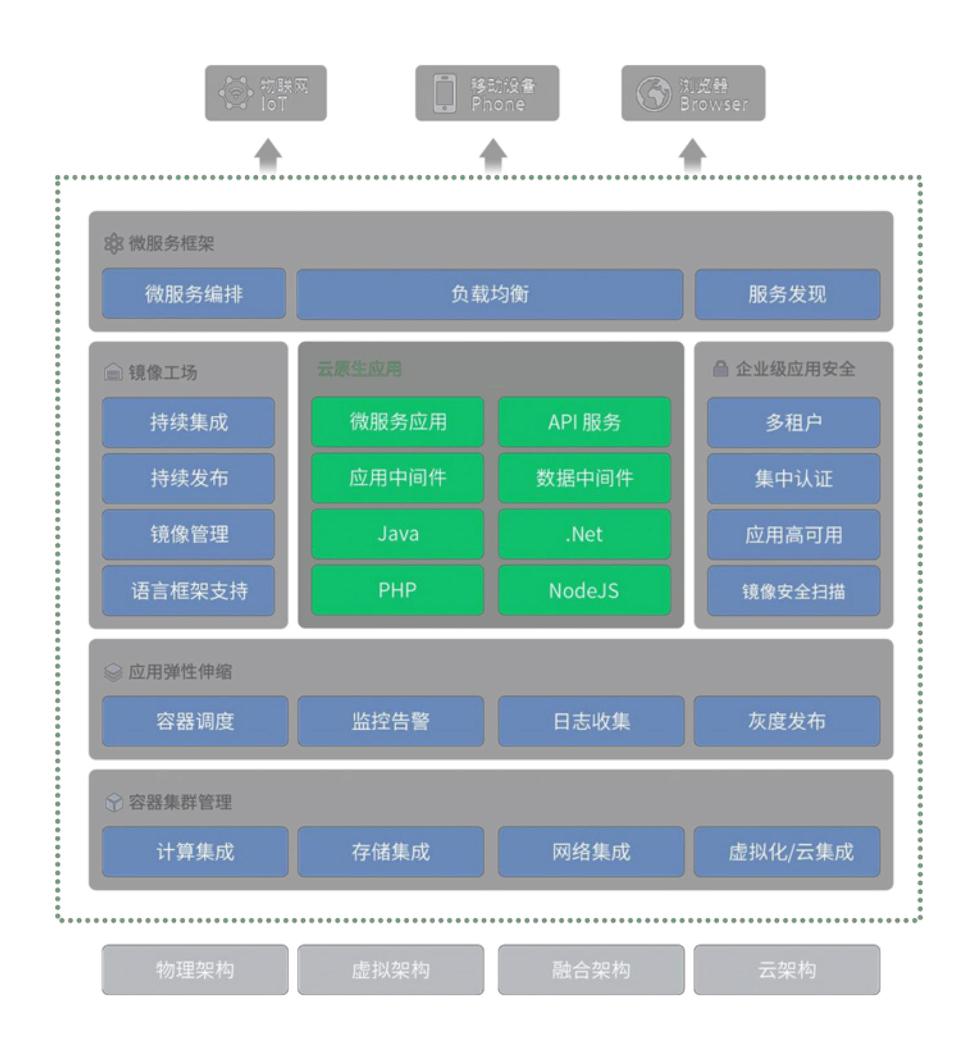
7.1 物理部署架构

云原生应用平台节点分为控制节点和运行时节点。管理节点负责平台整体的控制和管理，通过部署多台控制节点实现平台管理平面的高可用。运行时节点负责接收调度指令，运行容器并为容器提供计算、存储和网络资源，节点规模可以根据承载应用的规模不断扩大。物理部署架构如下图所示：



7.2 逻辑架构

方案基于 SOA 的设计理念采用微服务架构，基于微服务的设计方法，实现了云原生应用平台管理系统内部各模块之间的松耦合，保证了云原生应用平台管理系统的可移植性和可扩展性。云原生应用平台管理系统总体架构如下图所示：



云原生应用平台由四个层次构成，基础设施层、服务层、应用层、访问层，每个层级都是相辅相成，环环相扣，各司其职 , 其中 :

- 基础设施层，即基础服务设施内容，该层级是混合层，针对这个层级平台需要有良好的向下与向上的兼容性，需要支持包括 Openstack、vSphere、AWS-EC2、Windows Azure、阿里云等 IaaS 层的公有和私有的资源之外还需要对传统的物理机进行很好的兼容。

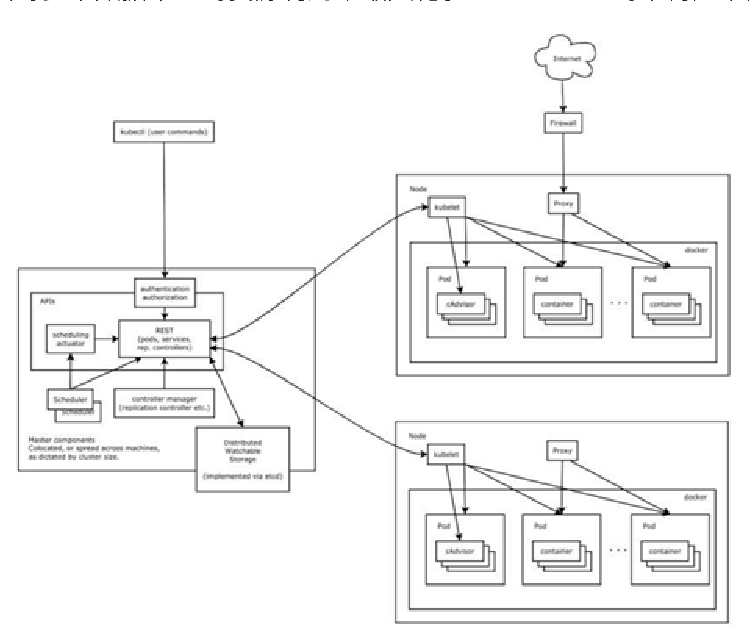
- 服务层，是应用市场核心层，平台提供应用模板、应用部署、容器 集群、 镜像工厂、主机管理、应用商店、存储定义、配置管理、平 台安全、平台 监控、弹性伸缩、可视化运营监控、微服务组件、标 准 SDK 及 RestFul API 等服务内容。

- 应用层，即容器服务层，提供容器化服务包含 : 负载均衡、弹性伸缩等，同时提供应用容器化的基础模板进行使用。
- 访问层，即使用户层，提供统一门户接入兼容为 PC、移动设备的访问， 基于 SDK 可以为业务提供良好的接入进行数据的交互。 服务层由应用管理、容器集群管理、镜像仓库管理、资源整合组件以及企业安全管理系统组成。平台遵循开源开放，提供所有功能 RESTAPI 接口，还可以将现有的周边系统接入云平台，供平台及应用使用。

7.3 容器编排

方案支持 Kubernetes 容器编排方案，帮助客户减轻技术决策 的风险，同时适配多样的客户场景需求。

Kubernetes 是一个以 Google Borg 为原型的开源项目，实现了资源管理的自动化， 以及跨多个数据中心的资源利用率最大化。Kubernetes 的架构如下图所示：

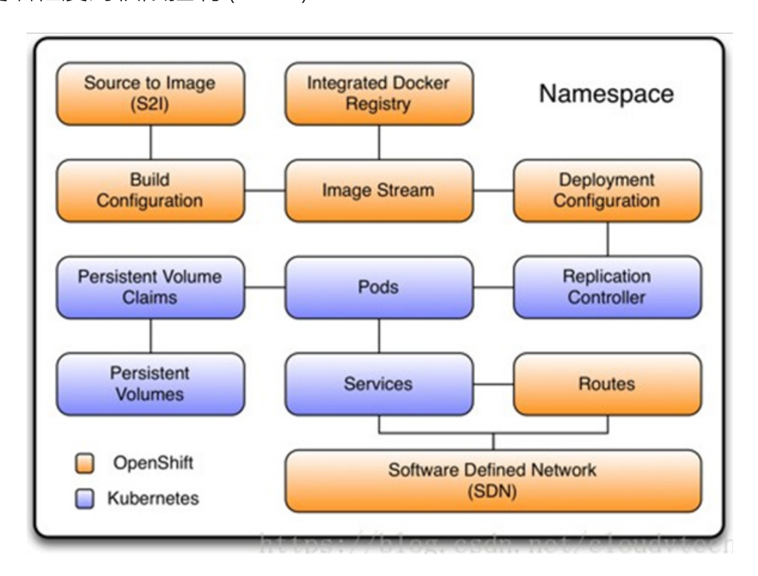


Kubernetes 提供完善的功能，相应的集群架构也更复杂，涉及到的组件比较多，管理和运维成本较高。所以比较适合于一些 IT 运维能力比较强的，同时对容器平台的功能要求比较全面的企业场景。

7.4 网络模型

OpenShift 可以看作是对于 kubernetes 和 docker 解决方案的更高级别封装，提供了 PAAS 解决方案级别的基础设施，包括：

- 镜像构建和 registry 存储
- 服务部署和暴露 (Router)
- 基于 OVS SDN 的 overlay CNI 实现
- 更细粒度的权限控制 (RABC)



在我们的应用向容器云解决方案迁移的过程中，在使用 kubernetes 方案作为过度之后，最终使用了 OpenShift Origin 作为容器云平台。

7.4.1 OpenShift SDN 基本概念

OpenShift SDN CNI 的三种模式：

- ovs-subnet：这种模式提供一个 flat 的 POD 网络，所有 POD 直接都可以相互通信。
- ovs-multitenant：这种模式通过 Virtual Network ID 在 OpenShift project

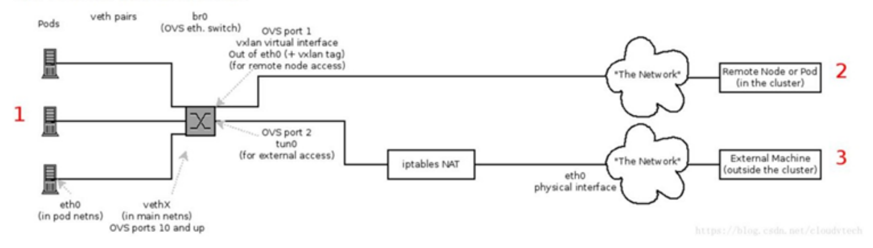
层面提供网络隔离，不同 project 之间的 POD 不能相互通信。

• ovs-networkpolicy：这种模式由管理员自定义网络控制策略进行网络隔离。

OpenShift SDN CNI 的节点：

• master 节点：监控节点加入事件，为新加入的 node 分配网络，在 etcd 进行注册；如果是 ovs-multitenant 模式，还需要监控 OpenShift project 的建立和删除来分配和删除 VxLAN VNID。

• worker 节点：向 master 节点注册并从 etcd 获取分配到的网络，并建立网桥 br0、OVS 端口 tun0 和 OVS VXLAN 设备 vxlan0 三个设备；POD 将 veth 对的一端绑定到 br0，tun0 提供 POD 访问外网的能力，vxlan0 通过 over layer 方式提供不同 node 之间 POD 的互联互通。节点还要监控新的节点和项目的增删事件，进行相应 SDN 的改变 (加减 subnet、加减 VNID 等) 。



7.5 存储规划

7.5.1 OpenShift 存储管理方案



存储资源是容器云平台中的一个核心基础设施，为不同的应用服务提供可靠的持久化服务。

大家都知道，容器运行过程中产生的数据是临时数据，并不可靠，一旦容器宕机，这些数据都会丢失。所以对数据可靠性有要求的应用就必须使用存储资源。

存储的方案有很多种，常用的有本地盘存储、NFS、Ceph、Gluster FS 等等。其中 Ceph 是一个开源的分布式文件系统，同时支持对象存储、块存储、文件存储，为云计算平台提供了最全面的存储方案。它以可靠、高性能等特性得到了很多企业的认可，并使用它来作为生产环境的存储。但是运维 Ceph 存储集群是一件较复杂工作，通过 Rook 项目，我们可以非常方便简单地实施 Ceph 存储方案，并且已有企业使用 Rook 来运维生产级别的存储方案。

Rook：CNCF 云原生存储项目

Rook 支持多种存储系统服务

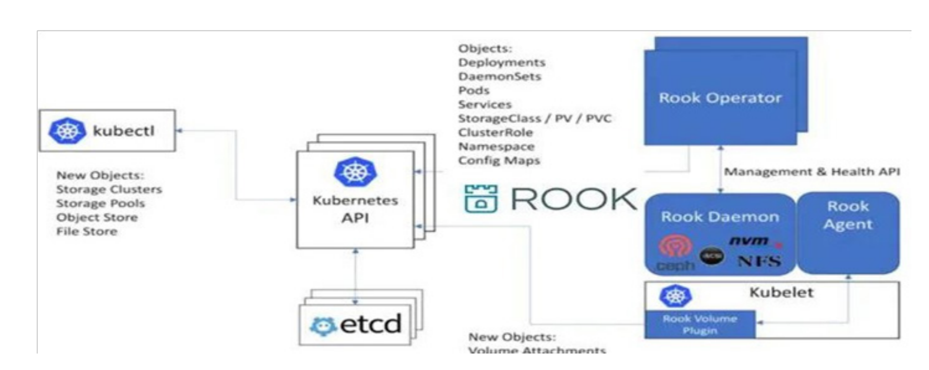
- Ceph（v1）
- EdgeFS（v1）
- Minio（Alpha）
- CockroachDB（Alpha）
- Cassandra（Alpha）
- NFS（Alpha）
- Yugabyte DB（Alpha）

7.6 Rook 的特性

- 简单可靠的自动化资源管理
- 超大规模或超融合存储集群
- 高效地分发和复制数据以最大程度地减少损失

- 通过多个存储提供程序配置，文件，阻止和对象
- 管理开源存储技术
- 轻松地在数据中心中启用弹性存储
- 根据 Apache 2.0 许可发布的开源软件
- 优化商品硬件上的工作负载

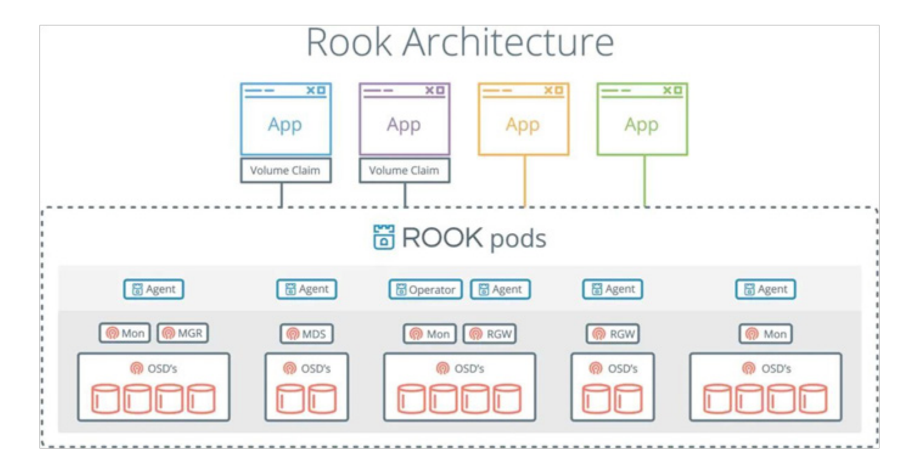
以下是 Rook 在 Kubernetes 上部署的架构：



7.6.1 OpenShift 容器平台部署 Rook

OpenShift 是红帽开发的 K8S 的企业级方案，它为原生 K8S 增加了许多安全及其他特性，特别是约束了运行中的 Pod 的权限。在部署与使用 Rook 时，需要允许应用拥有这些权限。

7.6.2 Rook 架构





8. 方案特点介绍

云原生应用平台旨在助力企业完成新一代互联网技术驱动下的数字化转型，实现全面软件定义的数据中心，加速业务的迭代交付，满足企业快速变化的业务需求。通过云原生应用平台企业可在已有 IT 基础架构之上实现 100% Docker 原生标准的「容器」集群，「DevOps」开发运维模式，标准化应用交付与流程化运维管控，安全可靠的自动化运维能力。以面向互联网「敏态 IT」的速度、规模和可靠性，管理日新月异的现代化企业应用和软件定义的数据中心。

8.1 云原生应用平台

作为云计算体系的重要部分，云原生应用平台提供了一种平台即服务功能以帮助使用者在无需关心底层复杂的基础设施情形下进行高效开发、运行和管理其应用程序。云原生应用平台服务厂商提供底层基础设施如服务器、存储、网络、虚拟机、操作系统、应用中间件及运行时环境，同时也提供相应开发套件和编程语言供开发者选择和使用，这样就将开发者有效解放出来并专注于上层应用开发。

8.2 容器技术标准化

作为一个容器技术，Docker 自从 2013 年开源以来得到了各大 Paas 厂商和开发者的极力支持并迅速成为容器领域的主流，进而成为近年来云计算领域中最热门也是发展最快的技术之一，相比其它 Paas 系统，Docker 有着如下显著优势：

- Docker 将容器技术标准化，提供标准的打包方式和交付标准，一次构建随处运行
- Docker 可实现应用在不同主机、不同系统、甚至不同云平台之间的流动和移植
- 相比重量级的虚拟机，Docker 非常灵活和轻量级，启动更快性能更 高，对系统资源的占用率也更低，这非常适合搭建企业私有 Paas 环境
- 方便构建 Devops 环境例如 CI / CD 集成环境、自动化测试等

鉴于以上特点和优势，Docker 正在重新定义 Paas 并已得到各主流 Paas 厂商平台的支持，同时 Docker 也帮助 Paas 拓展其使用范围：Docker 负责封装应用构建标准化交付容器，Paas 则提供运行时环境和云原生应用平台， 这样 Paas 既可承载上层各种 Saas 应用服务，也可服务于企业内部加速 DevOps 等应用体系的落地。

DCE 可以通过标准的方式来部署、管理、监控企业的 Docker 应用，并提供了容器，虚拟网络和存储的功能。DCE　是高度标准化的，基于 Kubernates。 DCE 提供了应用管理的功能，用户可以通过界面向导或者 YAML 文件来创建应用，并支持持续发布，审计日志等功能，还包含有容器环境，存储卷管理和虚 拟网络的功能。DCE 还提供了基于标准的镜像仓库，可以使用 内置的高可用仓库，也可以连接 Docker Hub 和用户的私有镜像仓库。

8.3 弹性伸缩

弹性伸缩（Auto Scaling）是根据不同的业务需求与策略，自动调整应用的弹性计算资源，最终达到优化资源组合的服务能力。通过自动伸缩和手动伸缩 这两种工作模式，应用便能在无运维人员介入的情况下实现自动调整计算资 源，当访问量上涨时增加计算能力，而当访问量下降时减小计算能力，既保障 了系统的稳定性与高可用性，又节约了计算资源成本。

弹性伸缩在业界有两个方向，一个是垂直化的扩展（Scale up），一个水平化的扩展（Scale out）。从业务发展的角度来看应该是水平扩展的能力，这要求业务都是无状态的，通过负载均衡技术将访问请求分配到集群每一台机器 上，不管是增加还是减少机器，业务的连续性都不应受到影响。

- 手自一体：自动扩缩提供指标扩缩和定时扩缩，搭配手动弹性扩展功能，实现对应用的手自一体快速、弹性扩缩，满足业务突发高峰时应用 的处理能力要求；
- 全场景：自动扩缩模块实现针对应用全场景指标的监控扩缩，比如应用 资源（CPU、内存）指标、应用自定义（Tomcat 连接数、线程数等）指标和七层负载均衡指标等，并支持对接 prometheus 指标；
- 生产级：支持只扩不缩，并提供扩缩前稳定性检查，扩缩中指标抖动的抑制，以及扩缩后事件记录。保证应用的稳定性访问。
- 低成本：流量降低自动缩容，避免资源浪费。

8.4 应用编排

支持 Kubernates 或 Helm Chart 应用编排，平台提供标准的应用编排规范，基于管理模板方式整合，把现有零散、复杂的应用进行碎片化拆分，然后可视化的



页面按照平台的标准进行整体应用编排。同时平台还支持：

- 支持应用编排模板的新建、修改及删除。
- 支持编排应用自动加入应用集群
- 支持应用模板的分类、搜索及筛选功能。
- 支持按租户管理私有应用模板和管理员提交共用应用模板，并支持将私有模板转化为应用模板。
- 支持 YML 格式开展应用编排，能够实时校验语法，出现错误时能报错，报错界面友好。
- 支持应用容器与外部资源的混合编排，如外部数据库、硬件负载均衡等。
- 支持单个应用下每个容器的信息查看，并可通过界面修改应用或容器配置。
- 容器信息应至少包含容器名称、IP 地址、端口、所属应用，应用版本，运行状态，所属主机等。
- 在应用管理模块内，支持单个容器的基本操作，包括创建、删除、启动、停止、重启等。支持容器的控制台（仿真 CRT 终端）访问，并支持终端内容的复制与粘贴。
- 可支持多维度的应用负载查看，如应用整体负载查看，应用中单个服务负载的查看，应用中单个容器的负载查看。查看内容至少包含 CPU、内 存、网络、线程数等。
- 支持对单个应用服务的不同运行版本进行管理。
- 灰度发布：支持自动灰度发布策略设置，能够设置每次更新发布的容器 数量，更新的目标比例等。

8.5 容器存储

容器运行期间产生的数据是不会在写镜像里面的，重新用此镜像启动新的容器就会初始化镜像，会加一个全新的读写入层来保存数据。如果想做到数据持久化，就必须寻求其他解决方案来保存数据。

容器云平台通过 ROOK 用于持久化存储 Docker 容器的数据， Rook 并不是自己开发一套存储方案，而是将现有的分布式存储系统云原生化，让它们能够实现自我管理，自我扩展，自我修复。 它使存储管理员的任务自动化：部署，引导，配置，配置，扩展，升级，迁移，灾难恢复，监视和资源管理。大大降低了存储系统的运维门槛，大大减少了维护成本。

Rook 支持多种存储系统服务，Ceph、EdgeFS、Minio、CockroachDB、Cassandra、NFS、Yugabyte DB。

Rook 的特性：

- 简单可靠的自动化资源管理
- 超大规模或超融合存储集群
- 高效地分发和复制数据以最大程度地减少损失
- 通过多个存储提供程序配置，文件，阻止和对象
- 管理开源存储技术
- 轻松地在数据中心中启用弹性存储
- 根据 Apache 2.0 许可发布的开源软件
- 优化商品硬件上的工作负载

8.6 集群高可用性

开箱即用的集群高可用性，无需共享存储等特殊基础设施，提供主从 管理节点方式无需刻意共享存储等特殊基础设施；采用主从管理节点的方式，集群状态信息高速同步，多处备份；可部署多个控制节点，部分控制节点异常停止后，其他正常节点仍然可对集群进行控制，结合容器达到高可用。

此项特性使平台具备高可用，从而保证了业务的可持续性，另外，降低了管理成本和难度，通过扁平化集群管理模式，多控制节点方式有效分担 管理压力，可实现超大规模的集群节点扩充。

Kubernates 进行集群管理，兼容性良好。对集群调度速度快， 可在千台以上节

点实现数万容器的灵活调度，并且能够全自动化，快速完成高 并发应用扩容。

由于 Kubernates 很好的实现了与 Docker 原生体系对接；弹性扩展节省了资源，保障服务正常提供，为支撑大规模高并发互联网应用提供了保障。

8.7 监控告警

云原生应用平台承担生产级应用的稳定性支撑，为保障平台及应用的可靠运行，需要搭建适合容器场景的监控告警平台。 监控平台通过对集群、集群内部组件、集群依赖的环境等关键监控点以及易发故障的监控点进行数据采 集，进而实现监控可视化展示、告警、通知、报表等功能来帮助运维人员及时准确的了解集群状态。

8.8 日志收集

日志是程序产生，并按一定格式（一般会带有时间）进行输出到文件或者终端的数据。日志按类型一般可分为：系统日志、应用日志、安全日志、设备日志，这些日志分散在不同主机或设备上。

在传统模式下，当需要对程序进行调试、故障排查等情况时，工程师需要远程登录到目标主机相应目录下，使用 grep / sed / awk / more / less / tail 等工具命令进行日志的分析处理。在单个文件较大、数量较多且分散在多 台机器时，查找出的数据需要聚合，效率会比较低下，有时还会错过重要线索。

因此，如果能把日志集中管理起来，并提供搜索和分析功能，不仅能提高故障排查效率，同时还能结合监控系统实时分析和掌握系统状态。

云原生应用平台可以通过与开源 Elasticsearch+Logstash+Kibana 对接，实现了日志解决方案，并提供以下特性：

- 多维数据分析模型及自定义化图表与视图
- 快速便捷数据检索
- 多平台支持
- 提供 BigData 级别的数据服务
- 便捷的横向扩展
- 开放性支持第三方集成

让用户能够及时并直观的获得应用运行情况，了解应用负载状态，并且可以通过日志查看便于定位问题的原因，减少服务中断时间，而通过配置文件支持自定义监控参数设定和报告生成；此外，支持提供完整的日志功能、具备可视化日志搜索查看、日志审计功能。

8.9 DevOps

打造符合互联网最佳实践的自动化 DevOps 研发流程。可以专注于业务创 新，持续推进产品升级，最终实现企业商业价值的不断提升。平台提供了持续 集成 (CI)、持续发布 (CD) 的能力。提交代码，触发 Devops 流水线执行 Build, Test, Deploy 等流程。释放研发团队持续创新的潜力，具体如下：

OpenShift 让用户可以创建、部署、管理云端应用，其云环境具体提供了磁盘空间、CPU 计算资源、内存资源、网络连接以及应用服务器。根据不同应用类型（数据库、编程语言等），OpenShift 会提供不同的文件系统布局（例如 PHP、Python、Ruby、Java）来创建不同的运行环境。此外，OpenShift 也提供了一定程度的 DNS（域别名）。

OpenShift 也为不同应用提供了临时文件存取（/var/tmp），超过 10 天没有被访问的文件将被自动删除。

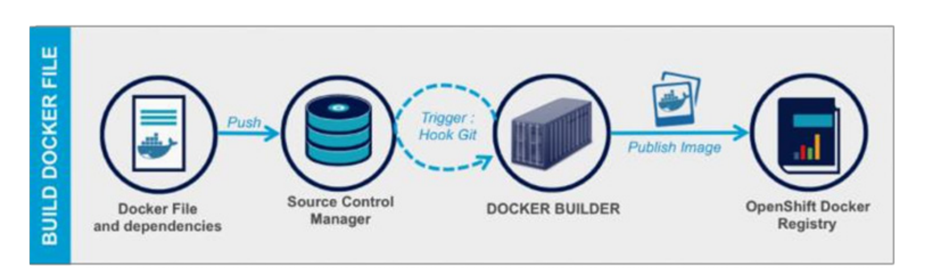
OpenShift 中包含两个基本的功能单元：

- Broker，提供了接口
- Cartridges，提供了应用框架

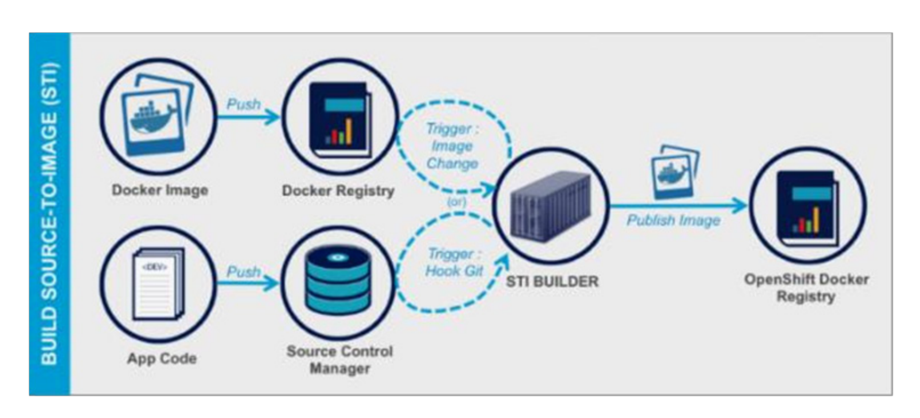
OpenShift 是由红帽推出的一款面向开源开发人员开放的平台即服务 (PaaS)。OpenShift 通过为开发人员提供在语言、框架和云上的更多的选择， 使开发人员可以构建、测试、运行和管理他们的应用。它支持用于 Java、 Python、PHP、Perl 和 Ruby 的更多的开发框架， 包括 Spring、Seam、Weld、CDI、Rails、Rack、Symfony、Zend Framework、Twisted、Django 和 Java E。它包含 SQL 和 NoSQL 数据存储和一个分布式文件系统。OpenShift Origin 是 OpenShift 平台使用的一系列开源组件。开发者可以利用这些组件搭建自己的 OpenShift 服务。

8.10 OpenShift 自动构建应用

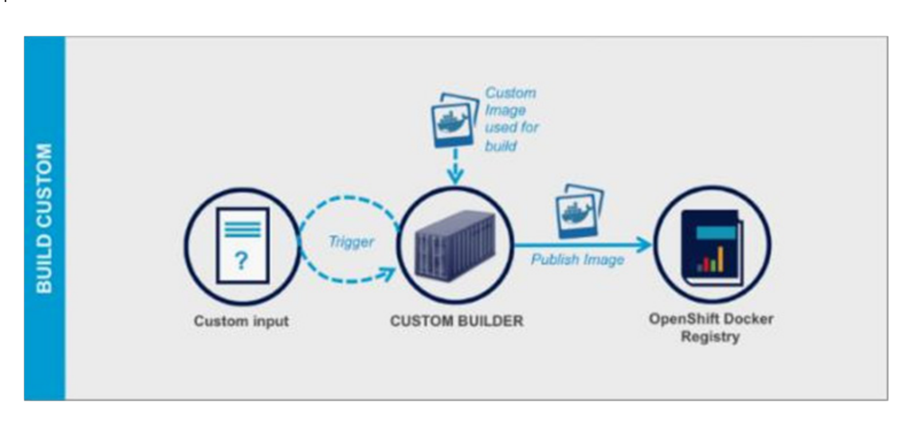
Docker 文件模式：通过向 OpenShift 提供指向 Docker-File 和它们的依附关系的源码管理器的 URI 来自动构建一个 docker 容器。



源码到镜像模式（STI）：允许通过提交应用的源码到 OpenShift 来自动构建一个应用。（就像 Heroku 中的 buildpacks）。

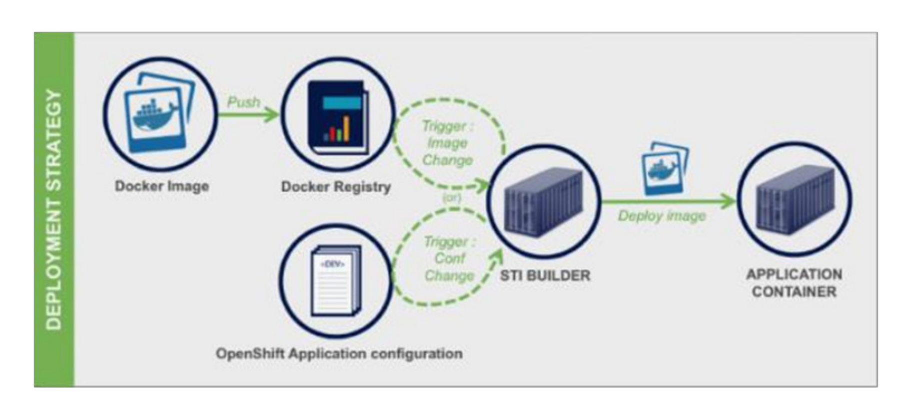


自定义构建模式：允许通过提供其自己的应用，其构建逻辑是通过提供 OpenShift, docker 的镜像。





OpenShift 也还允许定义一个自动的布署策略，比如有新的应用映像版本发布到注册表或者是应用的配置有了更新。



为了完成这些构建和布署特性，OpenShift 提供了把它自己的应用蓝图定义成用 Json 或 Yaml 格式的模板文件的功能。 这些蓝图描述了应用的架构拓扑和容器的布署策略。下面的图表描述了 openshit 中的 3 层应用是如何将不同组件的模板进行组合的。

OpenShift 是一个非常有前途的 PAAS 解决方案，它可以减少从项目开始时到自动构建应用和布署的时间， 它支持绝大多数的 WEB 架构， 即使数据的管理和外部服务的集成还没有完全应用。

平台对已部署的应用提供持续部署能力，提供自主定义的流程审批机制进行应用的发布根据实际情况执行发布流程，对已发布的应用提供应用版本管理，便于快速进行应用的切换回滚。

9. 关于上海天好

9.1 公司简介

探索实践 20 年，致力变革传统城市治理模式，推动跨领域创新应用，为可持续发展的中国助力！

经过二十年的发展，天好信息已成为一家综合性的信息化软件与服务提供商，不仅为政务、地产、金融等行业客户提供集应用软件定制开发、系统集成和相关运维技术服务于一体的信息技术整体解决方案，还为信息系统集成商和行业客户提供大数据支撑软件等软件产品和相关运维技术服务。

发展至今，公司已累计服务过全国 19 个省份的市、县、乡多个级别的政府机构、多家知名的证券公司、基金及资产管理公司等金融机构及房地产开发商，以及相关行业领域的信息系统集成商。公司 2011 年至 2016 年连续获得上海市明星软件企业称号，并于 2018 年荣获国家级创新软件企业称号、上海市软件企业核心竞争力评价（创新型）等荣誉，通过了信息系统建设和服务能力评估（CS3），取得了 ITSS 贰级、CMMI 叁级认证，取得了 ISO 9001 质量管理体系认证证书及 ISO/IEC 27001 信息安全管理体系认证证书。拥有 200 余项软件著作权和 8 项授权专利，已成为国内具备一定行业竞争力的软件企业和高新技术企业。

在软件业务领域，公司坚持“技术创新 + 基础平台 + 解决方案”的统一技术研发体系和产品开发模式，打造了基于组件化的软件开发平台和核心技术组合，形成了体系化、模块化的解决方案和系列软件产品。经过多年持续的研发投入与技术创新，公司在行业应用软件开发及大数据领域取得了丰富的技术成果，并在云计算、区块链、机器学习等新兴信息技术领域进行了前瞻性技术布局，通过不断创新研发、迭代优化，形成了集成开发平台（TP-DEV）、大数据开发平台（TP-DATA）、云智物联平台（TP-AI）三大软件开发基础平台及相关技术体系，能够灵活、快速响应不同的应用场景和需求，为公司软件开发提供标准、可复用的技术组件，实现公司软件产品的快速交付与稳定可靠运行，从而降低软件产品的开发运维成本。

在系统集成业务领域，公司凭借多年的市场积累和良好的服务意识，在政务和金融领域建立了比较稳定的客户群体，也逐渐培养了一支专业、高效的业务团队，具备成熟的集成整合能力和丰富的项目实施经验。

在运维技术服务领域，公司建立远程线上支持和现场维护相结合的服务机制，能够及时响应客户在软件升级、系统及硬件的调试与维护、故障排除与处理、设备更换、系统巡检及网络安全咨询及实施等运维技术服务需求。

在硬件销售领域，公司充分整合 IT 硬件及相关配套产品的供应网络，为客户提供全面的“一站式”采购服务，保障了高效、及时的产品供应能力。

未来，公司将依托多年来在政务、地产、金融等行业领域及大数据领域内所积累的技术、产品与服务优势，坚持“技术创新 + 基础平台 + 解决方案”的技术研发体系和产品开发模式，加大新产品、新技术研发力度，积极应对行业发展带来的新机遇和新挑战。在巩固已有市场基础上，公司将不断丰富以大数据、专有云、物联网等新兴信息技术为支撑的解决方案，围绕智慧城市及各大细分行业的信息化建设需求拓宽公司产品和服务的市场布局，进一步提升跨行业的应用开发能力。在未来三到五年内，公司力争发展成为国内领先的综合性信息化软件与服务提供商。

9.2 公司产品

智慧城市

- 政务服务与管理
- 产业投资与建设
- 工业大数据
- 民生惠民与运营

互联网业务

- 天好安心坊

智慧运维

- ITSM
- IT 资产管理
- 数据中心整体建设
- IT 外包服务

智慧房地产

- 采购招投标管理系统
- 供应商管理系统
- 成本管理系统

信息安全

- 等保咨询服务

9.3 公司主页

http://www.tele-hot.com/

10. 关于红帽公司

10.1 公司简介

红帽将协助为您的 IT 未来奠定更好的基础。我们使用 Red Hat® Enterprise Linux® 彻底改变了操作系统。现在，我们拥有广泛的产品组合，包括混合云基础架构、中间件、敏捷集成、云原生应用程序开发以及管理和自动化解决方案。

红帽提供强化的开源解决方案，使企业能够更轻松地跨平台和跨环境工作，从核心数据中心到网络边缘。通过透明和负责任的运营，我们将继续成为开源社区的催化剂，帮助您构建灵活、强大的 IT 基础架构解决方案。开放源码在过去、现在和未来将持续推动创新。这是世界需要的创新。这种力量超越了数据中心和新兴技术，并将创新掌握在每个人的手中。

红帽成立于 1993 年，在过去 25 年中，我们不断帮助客户应对业务挑战。超过 90% 的财富 500 强公司信赖我们，我们在 40 个国家的 100 多个地区为您服务。2012 年，红帽成为第一家收入超过 10 亿美元的开源技术公司。2019 年，IBM 以约 340 亿美元收购 Red Hat，这是历史上最大的软件收购。与 IBM 联手使红帽能够加强其现有的合作伙伴关系，为客户提供自由、选择和灵活性。

红帽是来自开源领域的领导者，现已成为 IT 领域的领导者。我们的开源解决方案



适用于世界上要求最严苛的数据中心和云堆栈。如今红帽不断在持续构建混合云、开发云原生应用和 IT 自动化方面助您一臂之力。

我们相信开放混合云的力量。基于专有技术的独立云部署阻止了云之间的交互。开放式混合云战略为混合企业环境带来开源软件的互操作性、工作负载可移植性和灵活性。

Red Hat 是 Linux 内核等开源社区项目的主要贡献者之一。红帽工程师帮助改进功能、可靠性和安全性，以确保您的基础架构运行并保持稳定——无论您的场景和工作负载如何。

精英管理、社区建设和透明度等开源价值观正在改变世界处理商业和生活的方式。红帽提供的工具、原则和标准为灵活性和创新奠定了基础。

10.2 发展历程

https://www.redhat.com/en/about/brand/standards/history